McGettigan Network Infrastructure

Hardware / OS / software:

- 16 ea Compaq Proliant 1800 and 3000 series servers used exclusively.
- OS: Windows 2000 Server & Windows NT Server SP6
- Databases: SQL Server 2000 & SQL Server 7.0
- Firewall software: Microsoft Proxy Server 2.0

WAN:

- Dual 512Kbps frame relay circuits w/ dual ISDN backup

Telephone System:

- Siemens 9005-9751 Model 50, Redundant CPU, Software bind 9005.6.84, two cabinet, eight shelf, 50 trunk lines, 2 T1's

McGettigan Web Technology Infrastructure

Hardware / OS / software:

- Dell 1550, 2300, 2450, 2550 servers used exclusively; standard configuration for servers: dual 1Mhz processor, 1Mb RAM, ultra SCSI HD
- OS: Windows 2000 Advanced Server SP3
- Database: SQL Server 2000 Enterprise SP2
- Web Server: IIS 5
- Firewall software: Microsoft ISA Server

Hardware distribution:

McGettigan Web Sites:

- 1 primary web server dedicated to McGettigan Web sites (McGettigan.com, McGettiganSolutions.com and customer specific sites managed by McGettigan Partners)
- 2 shared failover web servers in primary data center
- 2 shared standby web servers in alternate data centers
- 1 primary instance of SQL Server 2000 Enterprise dedicated to McGettigan web sites on shared high availability database server
- 2 shared failover SQL Server 2000 Enterprise database servers in primary data center

- 2 shared failover database servers in alternate data center
- Global load balancing between primary and alternate data centers
- 1 shared primary firewall
- 1 shared failover firewall

Meeting Operations Center / Physician Payment System

- 2 dedicated primary web servers
- 2 dedicated primary SQL Server 2000 database servers
- 1 dedicated storage array
- 1 dedicated standby server in alternate data center
- Global load balancing between primary and alternate data centers
- 1 shared primary firewall
- 1 shared failover firewall

McGettigansolutions.com Technology Overview

McGettigansolutions.com – Content Management Portal

Security

Physical

Primary Location, Netaxs in Conshohocken, PA: The Internet Data Center is locked 24 hours a day, 7 days a week. Outside door to Internet Data Center requires Magnetic Card & PIN for entry. The person seeking entry then must pass a 24-hour guard who requires photo id for positive identification and entry of identifying information in log book administered by the guard. Magnetic Card & PIN are required again for entry to actual Internet Data Center. All servers are locked in cabinets within the data center. Server cases and faceplates are locked to restrict access to hard drives. BIOS restrictions to prevent unauthorized use of removable media and I/O devices are implemented wherever possible.

1st Standby Location: "Warm" standby servers are maintained in IT4 Group's office facility in Gladwyne, PA. The outer doors to the building are locked 24/7. The office doors are locked 24/7. Access to IT4 Group's workspace is limited to IT4 Group personnel. A burglar alarm system is in place. No servers are left unattended in the logged-in condition under any circumstance. Contractors or other temporary employees are not permitted to work in the building or Office spaces unless accompanied by a full-time IT4 Group employee for the duration of their work there. Exceptions to this provision must be approved in writing by an officer of IT4 Group. Visitors must have an IT4 Group employee escort at all times. All sensitive data is encrypted. Server cases and faceplates are locked to restrict access to hard drives. BIOS restrictions to prevent unauthorized use of removable media and I/O devices are implemented wherever possible.

2nd Standby Location: "Cold" servers are maintained at a secure hosting facility in Atlanta, GA. No sensitive data is stored on this server, however it can be activated remotely by IT4 Group within one hour.

Network

- Inappropriate requests arriving via the internet are rejected by the firewall
- Portal members are authenticated by the PointSpace User & Group application
- Portal administrators are authenticated by Windows 2000 Advanced Server and the PointSpace User & Group application

McGettigansolutions.com
Technology Overview

Meetings Operation Center (MOC)
Data Repository

Security

Application

The **Meetings Operation Center** and **Data Repository** security schema utilizes positive security rights. A user must be defined and given certain rights in the systems in order to perform functions. There are several levels of security within the system to protect data from unauthorized access from with in an organization. In addition to the various levels of group access, each Client's data is contained in a stand-alone SQL Server database to protect from the possibility of unauthorized access from outside of an organization.
The **Meetings Operation Center** and **Data Repository** employs the use of temporary cookies on users' workstations that expire at the end of the session.

Physical

Primary Location, Netaxs in Conshohocken, PA: The Internet Data Center is locked 24 hours a day, 7 days a week. Outside door to Internet Data Center requires Magnetic Card & PIN for entry. The person seeking entry then must pass a 24-hour guard who requires photo id for positive identification and entry of identifying information in log book administered by the guard. Magnetic Card & PIN are required again for entry to actual Internet Data Center. All servers are locked in cabinets within the data center. Server cases and faceplates are locked to restrict access to hard drives. BIOS restrictions to prevent unauthorized use of removable media and I/O devices are implemented wherever possible

Network

Inappropriate requests arriving via the internet are rejected by the firewall

For Analysis Services (OLAP Cubes) –

- Client computers must have a freely distributable OLAP client component installed, which is named Pivot Table Services. This is installed by running PTSFULL.EXE found on SQL Server 2000 Enterprise Edition CD. SQL Standard Edition does not support OLAP services. Note that this has language dependent modules - the USA version will not necessarily work in another country.

For Analysis Services Embedded in Web Pages –

- ActiveX controls must be enabled and permitted.
- Microsoft Office Web Components must be installed on client machines to use SQL Server Analysis tools over the web. This is shipped with Office 2000 or above, both standard and professional editions. These components are not freely distributable. One needs to have a client license, or in other words, installed Office 2000.

- Browser security option for the Internet must permit "access data sources across domains" with either enable or prompt.

For Analysis Services Outside of Web Pages –

- **NO** ActiveX controls are used on the client.
- There are several products which can attach to the OLAP cubes on the remote SQL Server 2000 server via the Internet. They use the same Pivot Table Services as the embedded web components above. Two are listed below. Each connects to the remote

  data source via the Internet without the use of a browser. Each lets the user save favorite templates in file folders for repeated usage.
  - Microsoft Excel 97 or later

  OR
  - Microsoft Data Analyzer

McGettiganSolutions.com

The Meeting Portal

Documentation

Table of Contents

Basic description	3
Users, Groups, Communities and Permissions	4
Content Management and Link Management	5
Single Sign On (SSO)	6
Portal Administration Tasks	7
Portal User Tasks	9
Definitions	10
Troubleshooting and Reporting Problems	12
Minimum Requirements	14

McGettiganSolutions.com
The Meeting Portal

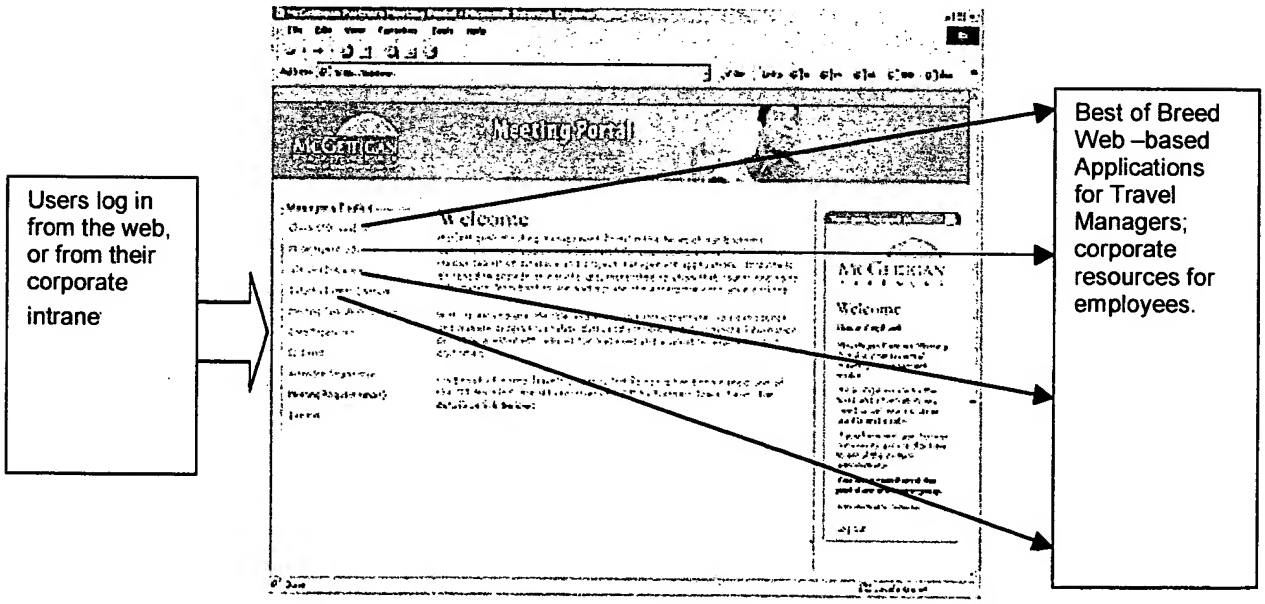
Basic description

The portal provides a means with which McGettigan Partners can offer its customers a comprehsneive toolkit consisting of best-of-breed web applications.

The portal makes it easy for Meeting Managers to log in once, even at their corporate intranet, and be logged in thoughout interaction with the Meeting Operations Center, the Physician Services Program, b-there.com, Ezevent, Starcite and a host of others. This technology is called Single Sign On (SSO).

The portal also makes it easy for administrators to manage content, links, communities, groups and individual users, without needing technical assistance from IT staff, web developers, or outside agencies.

The portal helps McGettigan Partners provide the best in customized technolgy solutions to customers, while at the same time simplifying the management of the the portal that ties the customers to McGettigan's and partners web applications.



As McGettigan Partners and it's suppliers create innovative new web applications, they can be added to the portal easily and quickly, by people with little or no technical training.

Users, Groups, Communities and Permissions

The portal is designed to provide a unique and very useful experience for each person who is a registered user. A registered user is someone whose information has been put into the portal by their site administrator.

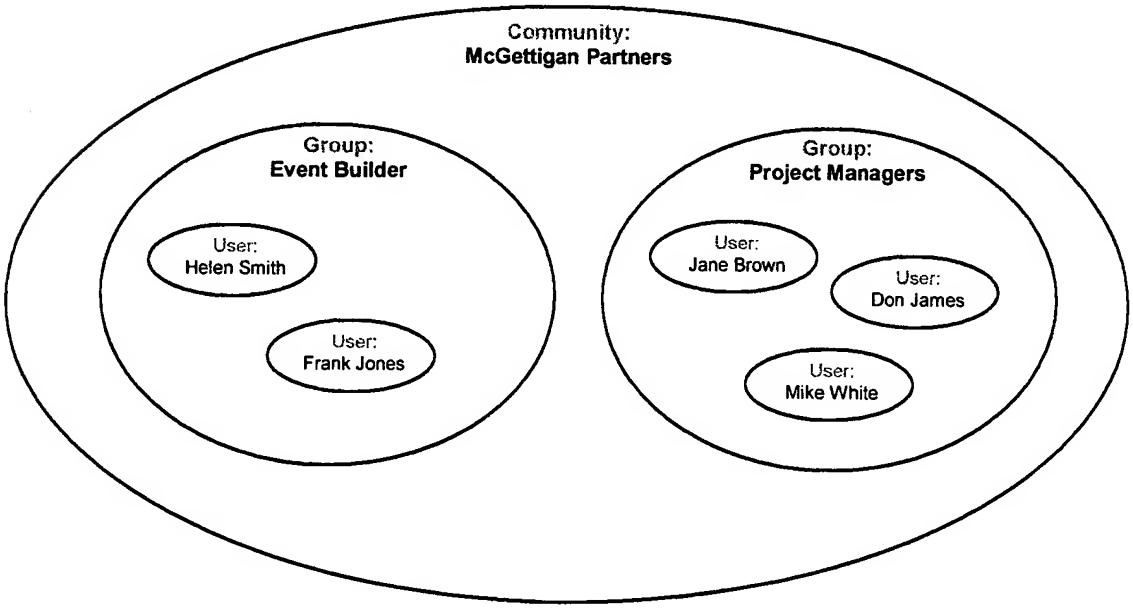
Once a person is authenticated by the portal – logged in, or otherwise recognized – the portal displays the links and content that have been made by the site administrator just for that person, the person's group, and the person's community.

A Way to Organize and Manage Custom Content

The primary reason behind dividing the world of portal users into communities and groups is to improve the site administrator's effectiveness in providing content and links customized for individual users who are part of large, diverse audiences.

The world of portal users consists of the following entities:

1. **User**: An individual person who visits or uses the portal. Users belong to groups.
2. **Group**: A collection of individual users who share a common characteristic, and also belong to the same community. A group may be a department within a company, a region of a country, a dialect of a language. Groups are part of a community.
3. **Community**: A group of groups that share a common characteristic. A community may be a company, a country, a language, or any top-level division that helps you organize your portal users in to easy to manage groupings.



How Authentication and Permissions Work

Authentication is the process by which an anonymous user becomes identified to the portal.

The most common form of authentication is the username and password, which are entered into a form on a log in page. Other forms of authentication at the portal include Single Sign On in which a user clicks a link on another web site, such as a corporate intranet, and is automatically logged in to the Meeting Portal.

There are three levels of identification that occur when a person logs in:

1. A username and password identifies the person
2. The person belongs to a group of people who will see similar content and links
3. The group belongs to a community of groups that share a common characteristic (same company, language, etc.)

The links and content displayed to the person after logging in are generated based on permissions set by the site administrator. Permissions are managed by the portal in the order listed below:

1. *Are there custom links and content objects authorized just for this USER?* Yes, display them and proceed to step 2. OR No, proceed to step 2.
2. *Are there custom links and content objects authorized just for this user's GROUP?* Yes, display them and proceed to step 3. OR No, proceed to step 3.
3. *Are there custom links and content objects authorized just for this user's COMMUNITY?* Yes, display them. OR No, nothing to display.

A user can have content and links that only that user sees. A user can have content and links that only that user's group sees. A user can have content and links that only that user's community sees. A user can have any combination of these. In most typical portals, the user would see links and content authorized for his or her group.

Content Management and Link Management

A web site consists of content – text, pictures, graphics and multimedia – and links to other web pages and web applications.

[screen captures and instructions will be placed here]

Single Sign On (SSO)

[screen captures and instructions will be placed here]

Portal Administration Tasks

[screen captures and instructions will be placed here]

Definitions

Administrator: A person who has been authorized to create, modify and delete some or all data in a portal. Data in the portal includes content, links, users, groups and communities.

Administrative Console: The screen on which an Administrator can view the communities, groups, users, links and content objects under their management.

Anonymous: A user that has not logged in or otherwise been authenticated. User Anonymous is a member of the Public group, which belongs to the Public community. All users, if not authenticated by the portal, are considered to be an Anonymous user, who belongs to the Public group, which is part of the Public community. Content and links created for the Anonymous user will display to anyone who visits the portal, until they are authenticated and custom content is displayed for them.

Authenticate: The process by which a registered user becomes known to the portal. Authentication can take place when a person enters their username and password, or it can take place automatically through the use of cookies or single sign on (SSO) techniques.

Community: A group of groups that share a common characteristic. A community may be a company, a country, a language, or any top-level division that helps you organize your portal users in to easy to manage groupings.

Content: Text, pictures, graphics, sounds, animation or video that appear on a web page.

Content object: A specific item of content that can be created, displayed and edited apart from other content objects. A web page may be one content object, or a collection of content objects depending on the way your portal has been built. A text content object can range in size from a single character up to 1,073,741,823 characters. Non-text content objects can include graphics, pictures, audio, animation, video, documents and spreadsheets. The portal can contain and manage an unlimited number of content objects, however the initial configuration is usually set for approximately 100,000 content objects.

Control Panel: The screen on which an Administrator can view and edit the properties for specific communities, groups, users, links and content objects.

Cookie: A small text file stored on the user's computer, which is readable only by the web server that put the cookie there. Cookies typically contain coded information that the web server can use to identify and authenticate the person.

Group: A collection of individual users who share a common characteristic, and probably belong to the same community. A group may be a department within a company, a region of a country, a dialect of a language. Groups always are part of a community.

Link: A clickable item that displays on one web page, and upon clicking, redirects the user to another web page. A link can pass a user to another page within the same web site, a page on another web site, or another resource such as a Word document, a PDF file, or a spreadsheet. The portal provides the capability to create and manage links that also pass authentication information out when clicked. This is called Single Sign On (SSO). SSO is used to pass an authenticated user into an external web site or web application already logged in, without having to enter a username and password for the external resource.

Public: The name of both the default community and its only default group. The Anonymous user belongs to the Public group, which is part of the Public community. All users, if not authenticated by the portal, are considered to be an Anonymous user, who belongs to the Public group, which is part of the Public community.

Secure Sockets Layer (SSL): A technology that encrypts the data that flows back and forth between your web browser and a web server. You can tell you have an SSL connection if the web address begins with "https" (note the "s" after the "http"), and you also see a small padlock icon in the lower right corner of your web browser. If you want to view information about the web server's security certificate, you can double click the padlock icon and explore the information in the SSL dialog box. The portal uses SSL to keep your information and your company's information private.

Single Sign On (SSO): The capability of a web site or web application to receive and/or send authentication automatically, saving the user the need to log in manually when linking between multiple web sites or web applications. The portal can receive and send SSO information. On the receiving side, the portal can automatically authenticate incoming users based on one or more of the following: an employee number or other single, unique identifying code; a cookie on the user's computer; an existing username and password being passed by another web site, such as a corporate intranet; a specific, unique referring internet address, such as a numerical IP address. On the outgoing (sending) side of the portal, authentication can be configured by site administrators to mesh with the receiving site's requirements. The standard SSO handler in the portal provides up to six unique identifying characteristics to be passed out with the click of a link on the portal.

User: An individual person who visits or uses the portal. Users can be known, or authenticated, by the portal, or they can be anonymous. Users belong to groups; groups belong to communities.

Troubleshooting and Reporting Problems

These procedures apply only to **McGettigan Partners Meeting Portal** and associated web applications at the following web addresses: **https://www.mcgettigansolutions.com** and **https://mpmoc.com**.

Any other web addresses encountered during operation of the Meeting Portal are not under McGettigan Partners direct control. See "Problem Reporting" for details of what to do if you have problems with non-McGettigan web addresses.

Always check the address window of your browser before using the following troubleshooting steps or reporting a problem. If the address in your browser does not contain the words:
"www.mcgettigansolutions.com" or **"mpmoc.com"**
these procedures do not apply.

Frequently Reported Problems and Quick Diagnostics:

Most problems reported to tech support personnel come under one of two categories:

1. Cannot connect to web site.
2. Functions are not working, including log in problems

Connection Problems:

The first category, connection problems, can occur at any one of the numerous points between your computer and the web server. The most common connection problem is at the user level – the local network is down, your network wire is loose or unplugged, etc.

A quick check of other web sites can rule out a user-level problem.

If *ibm.com, microsoft.com, yahoo.com* and *google.com* are not working, your internet connection is not working. Contact your supervisor or local system administrator for assistance.

If *ibm.com, microsoft.com, yahoo.com* and *google.com* are working in your browser, but the Meeting Portal at *https://www.mcgettigansolutions.com* is not working, your connection to the internet is working properly and problem is at the Meeting Portal web servers. Please follow the steps listed in the **Troubleshooting Guide** section below.

Frequently Reported Problems and Soluti ns: (continued)

Functi nal Problems:

The second category of problems, functions not working, may be caused by your browser settings, or they may be caused by your local area network and firewall settings, or they may be caused by problems in the web servers.

In general, if a function begins to work but gets stuck or returns an error message in a web page, the problem is most likely at the web server and should be reported immediately. (see **Reporting Problems**).

On the other hand, if your browser simply freezes up – certain functions such as buttons, links, forms and scrollbars stop working, or never work, the problem is usually in your computer or browser.

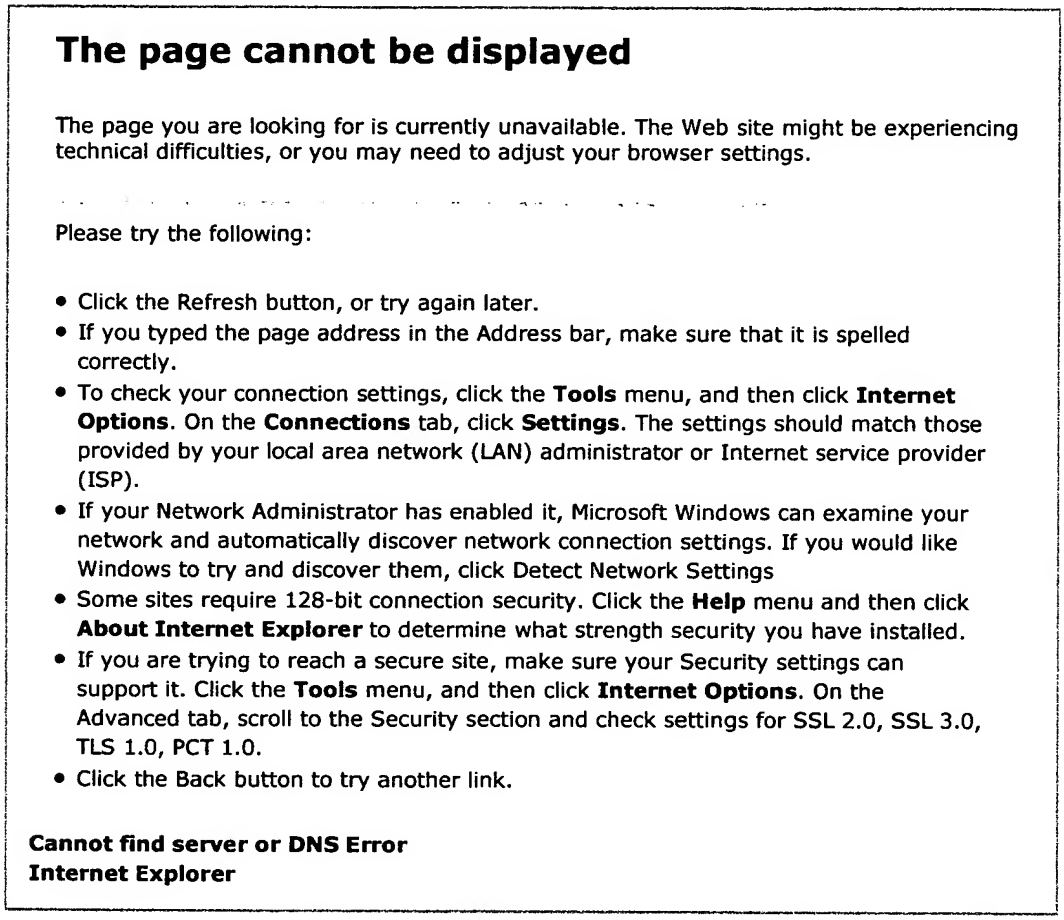
Many functional problems occur when a security setting in your browser prevents a web page function from operating. *Your browser security settings are part of your overall corporate security procedures. Do not adjust your browser's security settings. Please contact your local system administrator.*

Another source of functional problems occurs if you have too many applications or other browser windows open, which uses all available memory (RAM). In particular, pop-up windows and web sites with animation can tie up your system's resources if left open on your desktop.

A quick way to isolate a computer/browser problem is to restart your computer, then open one browser and try the function again. If it works, the problem was a memory lock up from too many applications or browsers open. If the problem remains, the most likely cause is a security setting in your browser, which should be reported to your local system administrator.

Troubleshooting Guide:

Contition: You cannot connect to the portal. You see an error page in your browser window that is similar to this:



The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically discover network connection settings. If you would like Windows to try and discover them, click Detect Network Settings
- Some sites require 128-bit connection security. Click the **Help** menu and then click **About Internet Explorer** to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the **Tools** menu, and then click **Internet Options**. On the Advanced tab, scroll to the Security section and check settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0.
- Click the Back button to try another link.

Cannot find server or DNS Error
Internet Explorer

Step 1: Check the web address you are trying to reach. It should read:

https://www.McGettiganSolutions.com

If the web address is correct and your connection still does not work, proceed to step 2:

Step 2: Close all browsers you have open. Open one browser again. Try a web address for one or more major high availabilty web sites such as **yahoo.com, ibm.com, google.com**, etc. If you ***cannot connect with these sites,*** your internet connection is not working. Contact your supervisor, system administrator or internet service provider (ISP).

*If you **can** connect with these sites, proceed to step 3:*

Troubleshooting Guide: (continued)

Step 3: Restart your computer and try once again to connect to **https://www.mcgettigansolutions.com**

*If you still **can** connect with other sites such as **yahoo.com**, but **can not** connect to **mcgettigansolutions.com**, proceed to step 4:*

Step 4: Try another computer in your department or company. Can you connect to mcgettigansolutions.com from another computer?

Yes → *proceed to step 5.*

No → *proceed to step 6.*

Step 5: If you can connect to mcgettigansolution.com on the other computer, try your own computer again. If you still cannot connect to mcgettigansolutions.com on your computer, proceed to step 6.

Step 6: Gather the following information: Date, time, steps taken, computers used during diagnostic steps. Go to **Reporting Problems.**

Note: The Meeting Portal at **mcgettigansolutions.com** is actually a system of several interconnected web servers and database servers located in geographically separate internet data centers on different segments of the internet. The primary servers have failover servers, and the primary internet data center has failover internet datacenters. It is very unlikely that all servers and networks would be unreachable In the event of a major network failure rendering the primary internet data center unreachable, traffic is automatically routed to the failover internet data center. During an actual failover event, a typical user might experience a temporary (approximately 1 minute) loss of connectivity.

Troubleshooting Guide: (continued)

Condition: You are connected to the Meeting Portal at **mcgettigansolutions.com** but a required function is not working.

Diagnostic:

Step 1: Are you logged in?

No → proceed to step 2.
Yes → proceed to step 3.

Step 2: Are you able to log in?

No → Have you ever been able to log in?

Yes → Can you log in from another computer?
Yes → The problem is with your computer. Contact your supervisor or local system administrator for assistance.
No → Check your username and password. If you are sure it is correct, see **Reporting Problems**

No → Is the log-in form working (submit button works)?
Yes → Record any error message displayed after clicking the submit button; see **Reporting Problems**
No → Contact your supervisor or local system administrator

Yes → Log in and proceed to step 3.

Step 3: Is only one function not working in the Meeting Portal?

Yes → Copy down the name of the screen, if appropriate, the time, date and a description of the problem. See **Reporting Problems.**

No → Does the browser window seem to be frozen?

Yes → Restart the browser. Does that solve the problem?
No → Restart your computer, then open one browser window only and try the the functions again. Does that solve the problem?
No → Contact your local system administrator.

No → Note the time and date, and write down all functions that are not working, see **Reporting Problems.**

Reporting Problems:

Before using any of the procedures below, please note that these procedures are for reporting problems – you can't connect to the portal or use the portal once you are connected.

Please be sure to follow the steps on the preceeding pages before escalating the problem using the procedures below.

Also, your supervisor or department may have internal problem reporting and escalation procedures in place. The problem reporting procedures in your business unit supercede these. Please check your company's problem reporting procedures.

[procedures worked out with McGettigan IT staff will appear here]

Minimum requirements:

To use the User functions of the portal:

Pentium 90 or better; Mac PowerPC, or equivalent processing speed

32 MB RAM minimum, although some browser functions may not work if the machine runs out of RAM due to load from other applications, incorrectly configured RAM, or incorrectly managed RAM.

Hard drive: No components or plug ins are installed. Web browser is only required application.

Windows 95-OSR2, 98, NT4, 2000, XP; Mac OS 8 or higher; other OS such as Linux and Solaris are not tested or supported, but may work satisfactorily.

640 x 480, 256 colors; 800 x 600, 16-bit color or better recommended.

IE 5 or above is recommended. Netscape 6 and 7 may work satisfactorily in most configurations, but are not supported for tech support purposes. Opera and other browsers are not tested or supported, but may work satisfactorily.

IE Security: All browser functions can be disabled or otherwise set to Maximum Security EXCEPT:

- "Cookies" > "Allow per-session cookies (not stored)" - set to "Enable" or "Prompt"
- "Scripting" > "Active Scripting" - set to "Enable" or "Prompt"

Non-IE Browser Security: Consult your system administrator to adjust your browser to allow Javascript to run and Session Cookies (non-persistent, non stored cookies) to be enabled.

Browser plug-ins and add-ons (Flash, ActiveX, etc.): None required.

Browser encryption stength: 128-bit required.

Helper applications; not required for portal but may be required for other resources referenced by the portal: Word, Excel, Acrobat

To use the Administator functions of the portal:

All specs are for Windows platform. Other platforms such as Mac, Linux and Solaris may work satisfactorily, but are not supported currently

Pentium 266, or equivalent, or better

64 MB RAM minimum, although some browser functions may not work if the machine runs out of RAM due to load from other applications, incorrectly configured RAM, or incorrectly managed RAM. 128 MB RAM or better is recommended.

Hard drive: No components or plug ins are installed. Web browser is only required application.

Windows 98, NT4, 2000 or XP

800 x 600, 256 colors (8-bit); 1024 x 768, 16-bit color recommended

IE 5 or above. Other browsers may work satisfactorily, but are not supported currently.

IE Security: All browser functions can be disabled or otherwise set to Maximum Security EXCEPT:

- "Cookies" > "Allow per-session cookies (not stored)" - set to "Enable" or "Prompt"
- "Scripting" > "Active Scripting" - set to "Enable" or "Prompt"

Browser plug-ins and add-ons (Flash, ActiveX, etc.): None required.

Browser encryption stength: 128-bit required.

Helper applications: None required

Server Environment Specifications

Data Exchange and MOC

Table of contents

1 Hardware and Software 2
1.1 Introduction 2
1.2 Deployment Architecture 2
1.3 Server Hardware 2
2 Server Configuration & Software Deployment 3
3 Checklist 7

1 Hardware and Software

1.1 Introduction

This document will list all the hardware, software and configuration components and their deployment techniques for a successful rollout of MOC application for McGettigan Partners (referred as MP henceforth). We will try to list the requirements at a detail level that is understandable and workable by a network and system administrator of a hosting farm to make a successful deployment.

1.2 Deployment Architecture

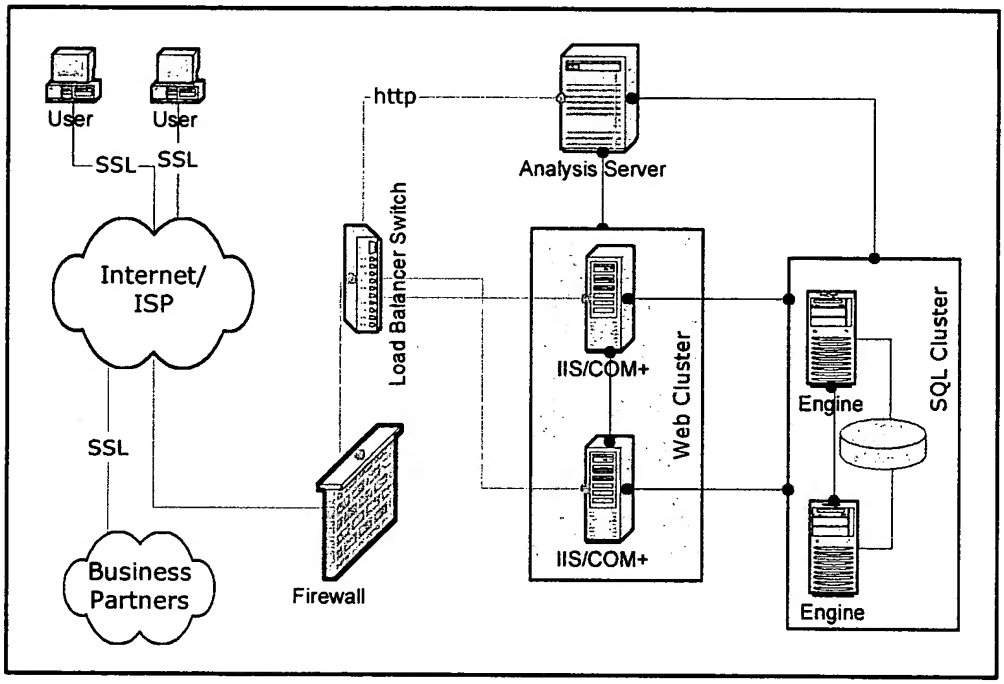


Figure 1

1.3 General Communication Guide

→ The web servers (in cluster) are accessed with http:80 and https:443

→ SQL Server should not be accessible from the internet except with Terminal Services.

→ SQL Cluster will be accessed using Named Pipes and TCP/IP:1443

→ The application account for SQL Server will have DBO permission on the following –

- All application databases
- ASP_Session
- Tempdb

→ The analysis server will be accessible from the web servers by HTTP and TCP/IP. However, this server should only be accessible by HTTP from the internet.

→ The analysis server will have additional local users under windows as required by the OLAP application. However, Analysis Server application configuration will be done by Data-Core directly at present.

ServerSpecification

1.4 Server Hardware

Type of Server	Specification
Web Server	Intel Pentium/Xeon based dual-processor server, 1 GB RAM, RAID-5 hard drives or approximately 40 GB space. To be optimized by McGettigan and/or Server Farm.
Database Server	Intel Pentium/Xeon based dual-processor server, 1 GB RAM, RAID-5 hard drives or approximately 20 GB space. To be optimized by McGettigan and/or Server Farm.
Storage Needs	SQL Cluster will need a fault tolerant Quorum drive as well as a shared disk array for data like EMC storage systems. Data space should be about 40 GB to accommodate growth in the near future. This will be extended in future as per need. To be optimized by McGettigan and/or Server Farm.
Analysis Server (SQL 2000)	Intel Pentium/Xeon based dual-processor server, 1 GB RAM, RAID-5 hard drives or approximately 40 GB space. Fast hard drive recommended.
Routers & Switches	Exact specifications for these components will be decided by the network administrator of the hosting farm or MP. They are not critical for this document as long as all the hardware devices are connected appropriately.
Backup & Recovery	Tape backup devices and media required for all the servers and the SQL data and transaction logs.

2 Server Configuration & Software Deployment

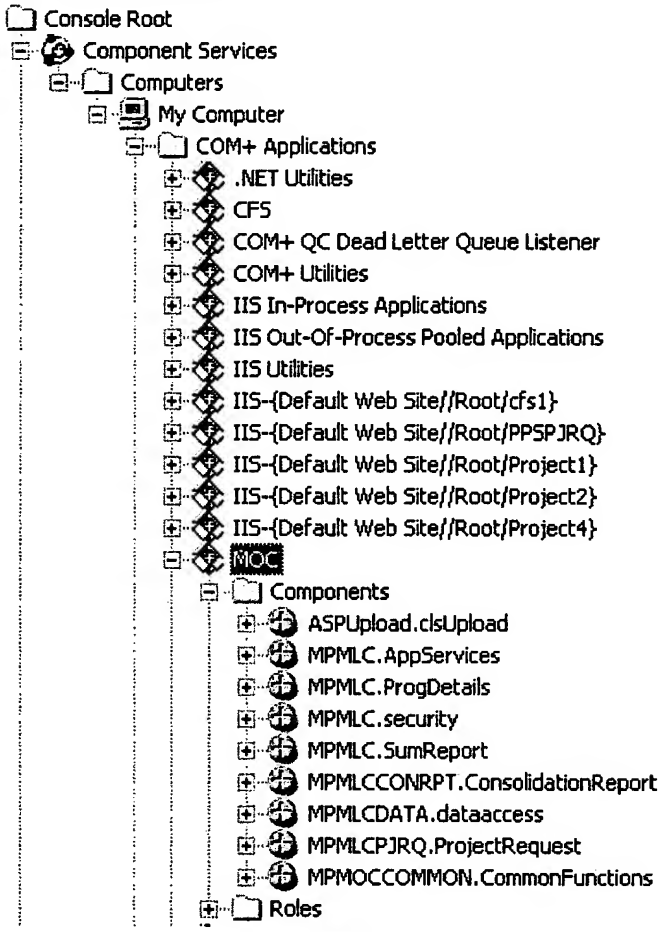
Purpose	Details
Firewall and DNS	**Two areas should be created for DMZ and Protected Network as shown in the architecture diagram. The DMZ servers are within orange shaded area and the protected servers are in the green shaded area.** **The registered URL should be resolved to the virtual IP address of the NLB cluster.** **The firewall must allow http communication on port 80 and https communication on port 443 to the web servers. In additi n, the firewall will also facilitate a VPN and Terminal Services connecti n to the web servers from clients originating fr m a limited number of known IP addresses.**
Web and Application Server	**→ Operating System – Windows 2000-based Servers. The**

ServerSpecification

Purpose	Details
	cluster nodes must be ASP Session Aware. This means, requests from a particular client must always g to one particular node. **→ The web servers also d uble-up as COM+ applicati n servers.** **→ IIS should be installed with web server FTP server and SMTP Virtual Server. SMTP Virtual Server on each of the web servers must be able to send email with anonymous authentication from inside the domain.** **→ An SSL certificate must be deployed on both of the web servers. The certificate must be issued to the registered domain common name, i.e., www.mpmoc.com and should be tested to be operating from both web servers.** **→ The latest version of Internet Explorer should be installed.** **Microsoft XML 3.0. This is freely downloadable from Microsoft site.** **→ Install Visual ASP Component Pack version 4.0. This is downloadable from www.viualasp.com site. Required licenses will be automatically deployed with application.** **→ SQL Server Client library must be installed.** **→ Microsoft Excel 2000 SR-1 or 2002. All Microsoft released service packs should be applied. No other components of Microsoft Office are required and they should not be installed. That will create unnecessary load on the server.** **→ Install Microsoft .Net Framework latest version.** **→ Install MDAC 2.7 SP1.**
SQL Server Cluster Nodes	**→ Besides cluster configuration, these two nodes will have the SQL Server 2000 Enterprise with latest service pack available from Microsoft site.** **→ The SQL Server cluster instance name should be resolved at the web servers by named pipes or TCP/IP with port 1433.** **→ The SQL servers will be in the protected area of the network. Only communication from DMZ will be allowed originating from the web servers through Named Pipes and TCP/IP.**
Microsoft Analysis Server	**→ This is a separate server for OLAP-based applications in MOC. This server will be accessed both from web cluster as well as directly from internet with http on port 80.** **→ The analysis server needs the SQL Server 2000 Client tools installed for application maintenance.** **→ SQL Server 2000 Analysis Services m dule will be installed n the designated server as shown in** Figure 1 **in**

Purpose	Details
	this d cument. **→ Install PTSFULL.EXE from the SQL Server 2000 Enterprise Edition Disk.** **→ This server sh uld have ports 80 (http) and 443 (https) open for internet access.** **→ Along with Windows 2000 Server, IIS must be installed on this server.** **→ This server must be able to connect to the SQL Cluster instance through TCP port 1433 for the SQL Cluster.** **→ This server is recommended to be in the same subnet as the web server cluster. The web servers will access this server through TCP ports.** **→ Check for the existence of a file "MSOLAP.ASP" at the IIS Default Web Site pointed physical folder on this computer.** **→ Open Internet Explorer and browse** http://localhost/msolap.asp**. This should result in a blank page and no error. This will confirm appropriate IIS configuration on this machine.** **→ Install Microsoft .Net Framework latest version.** **→ Install MDAC 2.7 SP1.**
Remote Access to the Servers	**Configure remote access for the web servers to facilitate the application development team to connect to the servers through a VPN and Terminal Services. The remote access may be turned on as Remote Administration Mode only so that additional licenses will not be needed. The default 2 connections are sufficient for our need.**
User Accounts	**There must be one Windows 2000 domain user account created for each of the following –** - **Terminal Services login ID for the development team. This ID must be a domain administrator.** - **Another domain administrator account that will be used for application services on the web/application server boxes in the NLB cluster. Disable terminal services access for this ID.** **An SQL Server user account is required that will be used by the application DSN. This SQL user name will be provided with "dbo" privileges on all the databases for the applications deployed on the application server.**
Web Server Application Deployment (identical steps for both the servers in NLB Cluster)	**→ Run the web application setup program from the deployment package.** **→ C nfigure the error pages as shown in** Figure 5: Custom Errors **at the end of this document.** **→ Run the COM+ Application Setup package from the deployment CD.** **→ COM+ C nfiguration – Now open Component Services**

ServerSpecification

Purpose	Details
	Administrati n window from start menu. The tree looks like the following –  **→ Again, right-click on "MOC" and open properties. Select "Identity" tab and specify the user as shown in** Figure 6: COM+ Identity. **The only difference will be the actual domain name in place of "DCSPROJECTS" and the application user ID created in place of "mcgapps" shown in the picture. This account is the second one described under the section "User Accounts".** **→ Follow the same steps for PPS deployment also.**
SQL Server Deployment	**→ First, follow the guide provided in the distribution CD.** **→ Make sure to delete any user from the database tree created as a result of database restore. Then provide the earlier-discussed SQL Server User ID a "dbo" access on the application databases.**
Virus Protection Software	**Install Norton Antivirus on all the servers.**
Backup & Recovery	**All the servers should have a complete backup and recovery system implementation. The web servers should have a c mplete data and system state backup. For SQL Servers a separate d cument will be prepared for backup and recovery as part of an overall operations guide.**

ServerSpecification

3 Checklist

After completion of all installation work here is a list for a quick check to avoid surprises –

- Default web site is started in IIS
- DNS resolves the default web site as www.mpmoc.com
- Latest service packs and release are applied as available from Microsoft Windows Update web site www.windowsupdate.com.
- Internet Explorer 6.0 with latest patches
- Terminal Services is configured and enabled for support team.
- SMTP Virtual Server is functional in both the web servers. They should be able to send email. If outbound emails need authentication, the id/password etc must be provided at the time hand-over.
- The DSN works.

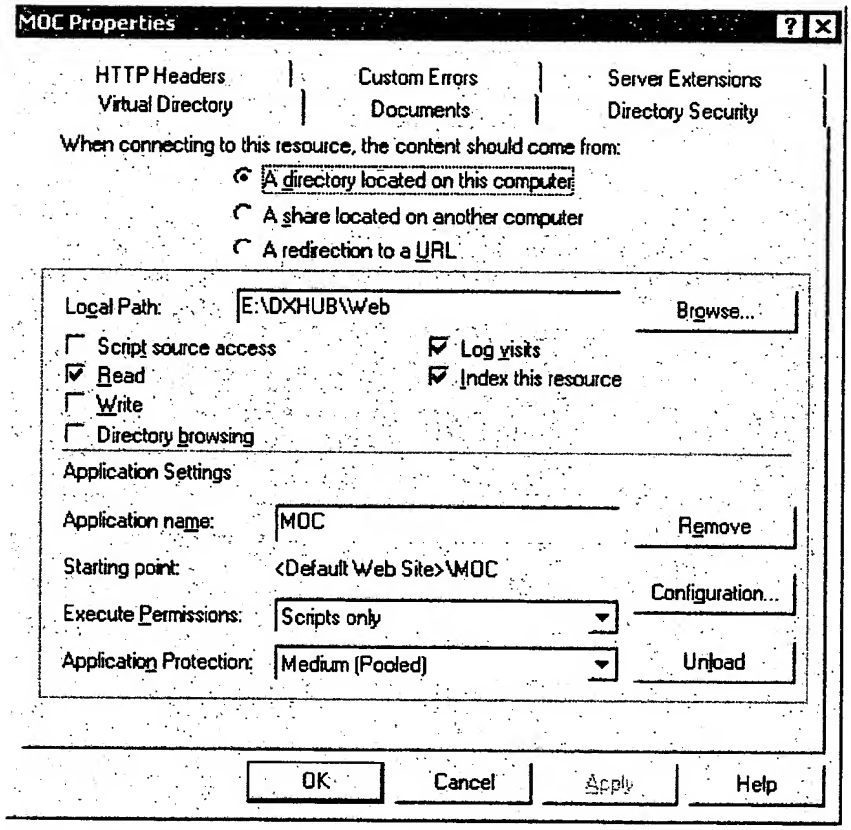


Figure 2: Virtual Directory

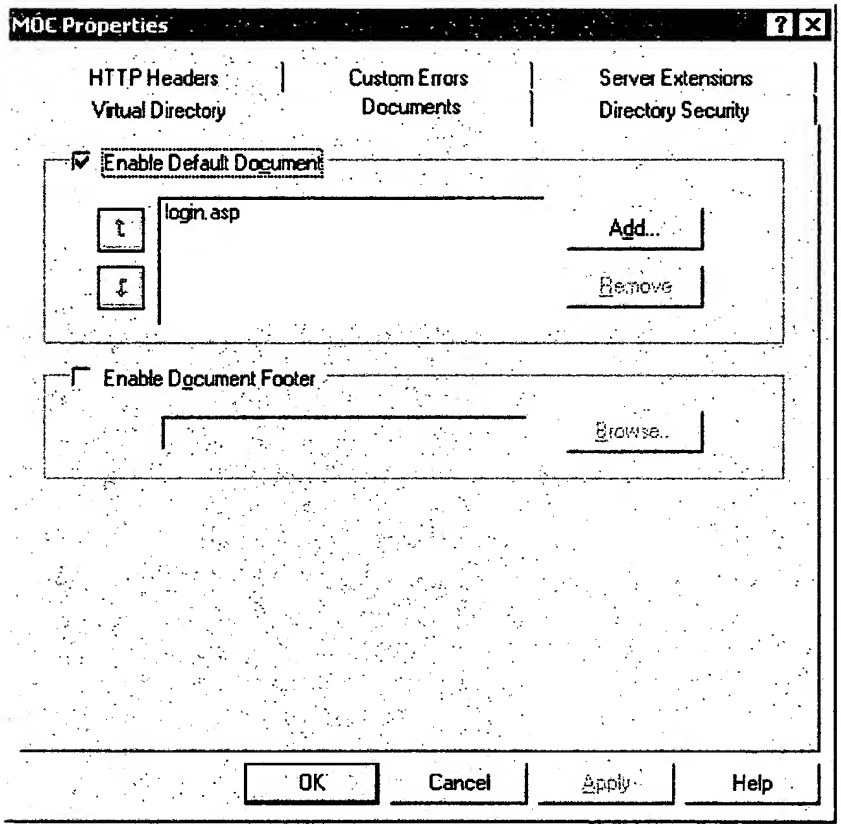


Figure 3: Default Document

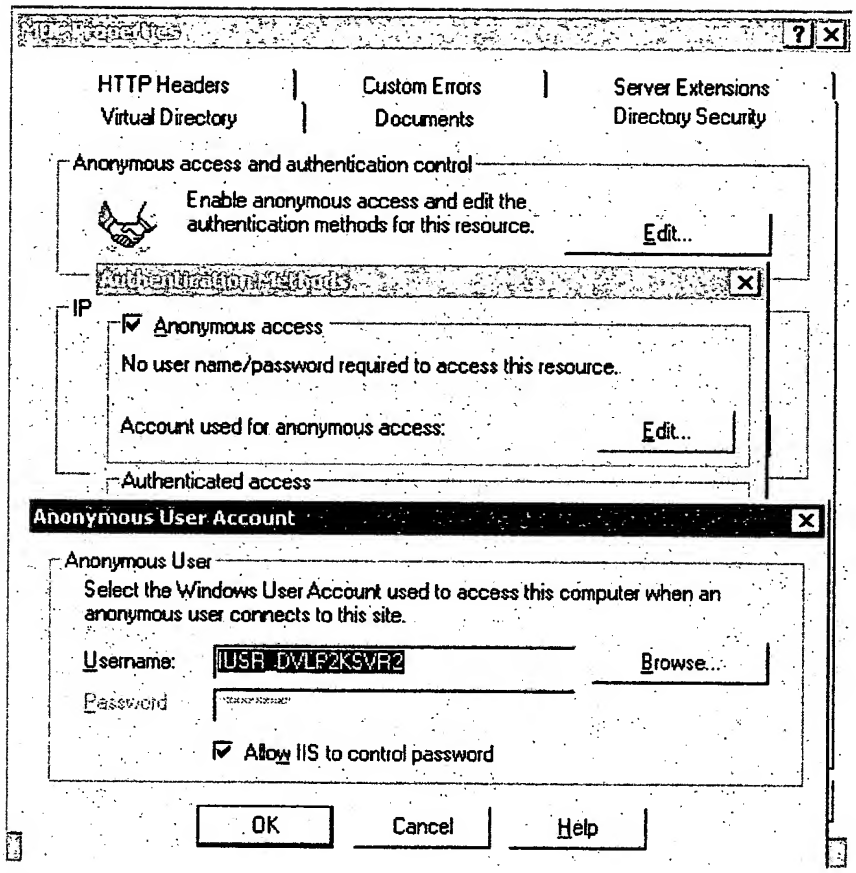


Figure 4: MOC Security

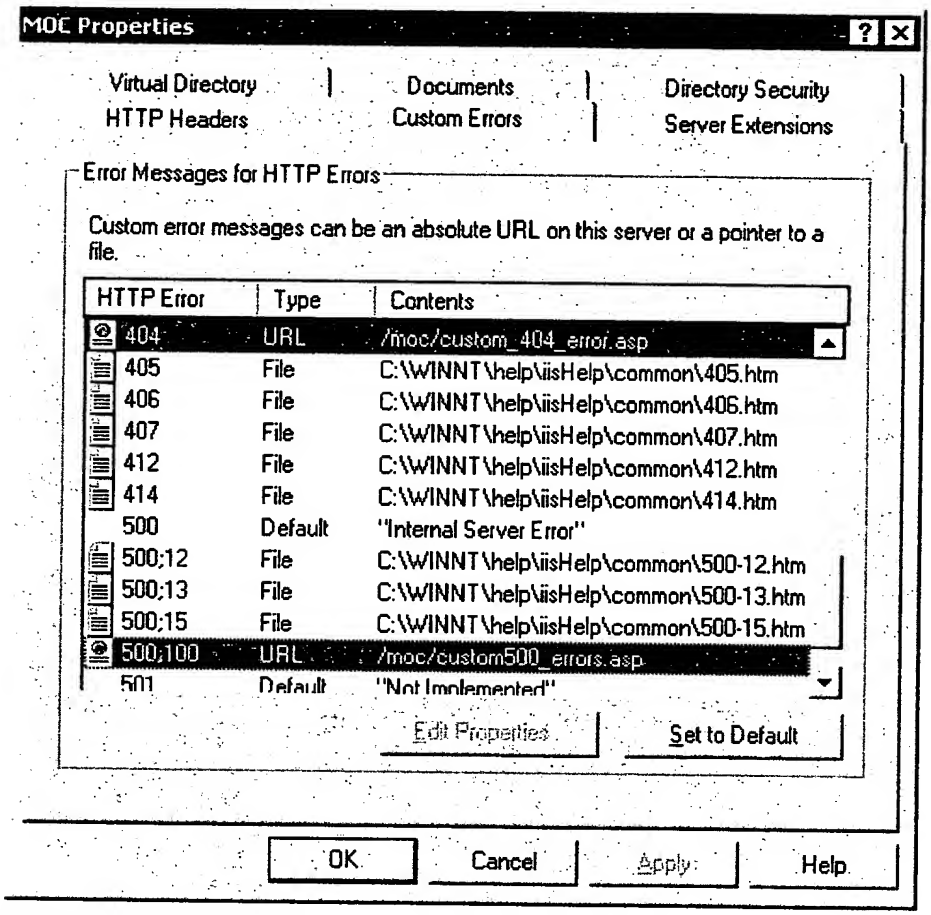


Figure 5: Custom Errors[1]

[1] The button "Edit Properties" will be available if you select one line at a time. In this picture, I have selected two lines together to explicitly show the lines that needs to be modified. The target type is URL in both the cases with full virtual directory path from the default web site root.

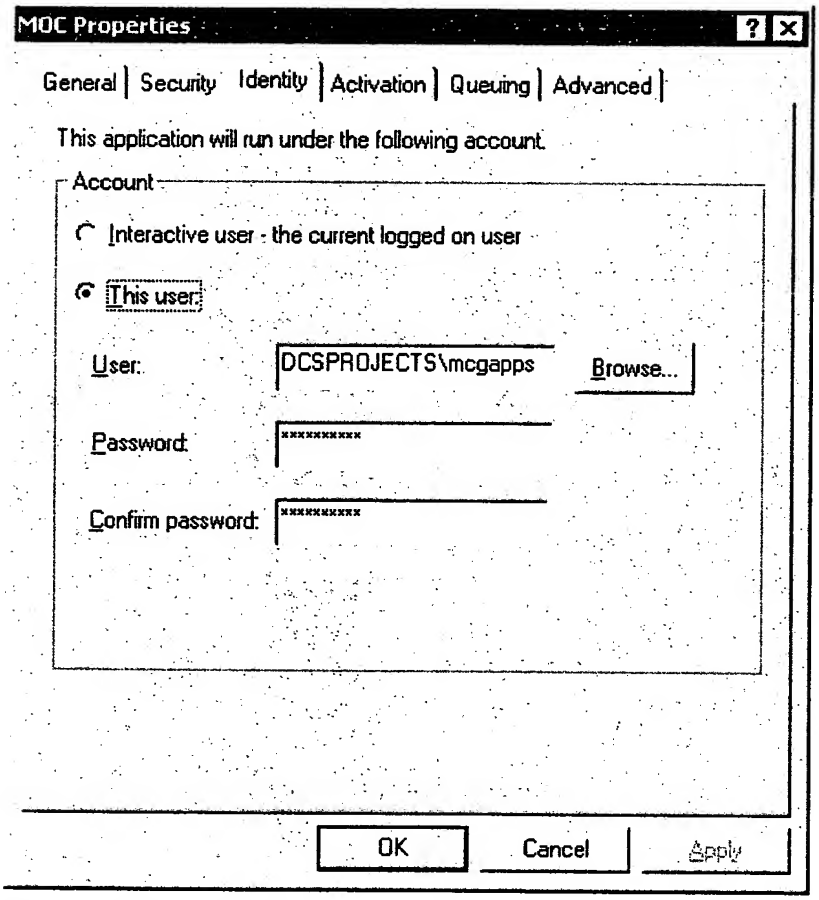


Figure 6: COM+ Identity[2]

[2] Note that the parameters in this picture reflects the way it is set up in the development environment. Use your own domain\user_id for the User field. This user must be an administrator to the computer.